U. S. Residency Certification (US CERT) – Privacy Impact Assessment

PIA Approval Date – Dec. 9, 2009

System Overview

The U. S. Residency Certification (U. S. CERT) is a client (thin)-server database application whose primary function is to generate Official IRS Form 6166 Letters. These form letters certify U. S. residency for those entities (individual, corporation, partnership, trust, estate, exempt organization, and employee plan) who wish to claim benefits under a tax treaty with or obtain exemption from a Value Added Tax (VAT) imposed by a particular foreign country. The Form 6166 letter(s) is consequently submitted with the foreign government's form by the taxpayer (or third party on behalf of the taxpayer).

Systems of Records Notice (SORN):

- IRS 22.028--Disclosure Authorization and U.S. Residency Certification Letter
- IRS 34.037--IRS Audit Trail and Security System

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer –
- Taxpayer Name or Business Name
- Name Control
- Social Security Number (if applicable)
- Address
- Taxpayer Identification Number (TIN),
- Foreign Address Indicator
- Phone Number
- Certified Name Line
- Applicant Type
- Form Filed or not Required
- Plan Number
- Type of Exempt Organization
- Certification Year
- Tax period
- North American Industry Classification System (NAICS) Code
- Tax Information Authorization
- Authorized Tax Forms and Tax Years
- Associate Listing
- Country Codes

B. Employee – The system captures information about employees' working in the system. The data elements include:
- Windows login
- Standard Employee Identifier (SEID)
- Operator Name and Number
- Team number

C. Audit Trail Information – U. S. CERT does not perform any auditing. The following events are audited through the supporting GSS (MITS–30):
- When the event occurred.
- The user initiating the event
- User name and SEID.
- Date and time.

D. Other – The Batch ID & Case is generated by the system. The Internal Revenue Service (IRS) Received Date, Inquiry Date, Correspondence Date, and Remarks are entered by the employee.

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

A. IRS – Name Control, Filing Requirements, NAICS Code, Filing Year Month, and Transaction codes are captured from the Integrated Data Retrieval System (IDRS) via an automated interface for purposes of verifying a taxpayer's U.S. residency based upon filing type and status.

B. Taxpayer – Paper Form 8802 applications containing:
- Taxpayer Name or Business Name
- Name Control,
- Social Security Number (if applicable),
- Address
- Taxpayer Identification Number (TIN),
- Foreign Address Indicator
- Phone Number
- Certified Name Line
- Applicant Type
- Form Filed or not Required
- Plan Number
- Type of Exempt Organization
- Certification Year
- Tax period
- NAICS Code
- Associate Listing
- Country Codes from taxpayers, or authorized entities operating on behalf of the taxpayer are input by IRS clerks and/or Tax Examiners into the U.S. Residency Certification database application.

C. Employee's
- Windows login
- SEID,
- Operator Name and Number,
- Team Number

D. Other Third Party Sources (Describe) –
- Form 8802, Form 8821, or Form 2848 provide Taxpayer Information
- Authorization and Power of Attorney data.
  o Third party's name
  o Third party's address
  o Tax forms subject to disclosure
  o Tax Years subject to disclosure

3. Is each data item required for the business purpose of the system? Explain.
Yes. Each data element is used to determine applicant's entitlement of benefits under a given Tax Treaty with a foreign country.

4. How will each data item be verified for accuracy, timeliness, and completeness?
Validation of each critical data item is performed at the input level to ensure that each conforms to a predetermined set of rules for data type, length, value ranges, format, and consistency. Validation is also performed at a record level to guarantee that all of the critical data elements are consistent as a whole and are viable for processing. Validation is completed through an automated interface with IDRS to ensure Taxpayer Identification Number (TIN) and Name Control match on the entity, filing requirements, filing type and status for a given tax period, and business activity codes (if applicable). The system utilizes a status code scheme to report to the user a case's completeness or lack thereof.

5. Is there another source for the data? Explain how that source is or is not used.
Yes. The Centralized Authorization File (CAF) system. Individuals can use the CAF system to supplement 8802 information. US CERT and CAF are not interconnected.

6. Generally, how will data be retrieved by the user?
Authorized end users (approved through OL5081) retrieve data from the system through a Windows–based graphical interface that connects to a backend SQL database.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. Data is generally retrieved by querying using a unique record identification number, but users have the option of also querying on the TIN, or the taxpayer's name.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?

Role: Users
Permission: Users are granted basic access to the data, with limited modification privileges as approved by their manager through the Online 5081 (OL5081) process.

Role: Managers
Permission: Full access to the data, but not the underlying database objects.

Role: System/Database Administrators
Permission: Open access to the data and the underlying database objects for data recovery.

Role: The Headquarters, Planning & Analysis and Program Analysis System analysts
Permission: Read–only access to the data.

9. How is access to the data by a user determined and by whom?
IRS personnel requesting access complete an OL5081, Information System User Registration/Change Request. Access to the data is determined by the manager based on a user's position (role) and need–to–know. Criteria, procedures, controls, and responsibilities regarding access are documented in the Information System Security Rules on Form 5081 (Information System User Registration/Change Request).

10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared.
Yes. Data from IDRS (Integrated Data Retrieval System) on masterfile (IMF, BMF, and EPMF) is extracted by an automated interface from USCERT. The elements collected are:

- Name Control
- Filing Requirements
- NAICS Code
- Filing Year Month
- Transaction codes

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
Yes.

Integrated Data Retrieval System (IDRS)
- Authority to Operate (ATO) – March 10, 2009.
- Privacy Impact Assessment (PIA) – November 6, 2008

12. Will other agencies provide, receive, or share data in any form with this system?
No. Other agencies do not provide, receive, or share data in any form with U. S. CERT.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
Output (U. S. Residency certificates) is not retained by the IRS. However, The paper Form 8802 is retained for six years and three months after the calendar year in which the case is closed. System records are retained on–line for 18 months after a case is closed and archived off-line for 10 years. See Request for Records Disposition Authority (Job # N1–058–08–4), IRM 1.15.29, Item 4 signed by the Archivist of the United States.

14. Will this system use technology in a new way?
No. U. S. CERT does not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
No. U. S. CERT is not used to identify or locate individuals or groups. The purpose of this system is to provide certification of U. S. residency for tax purposes to the taxpayer for his or here use.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.

No. U. S. CERT does not provide the capability to monitor individuals or groups. The purpose of this system is to provide certification of U. S. residency for tax purposes to the taxpayer for his or here use.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?

No. U. S. CERT does not allow the IRS to treat taxpayers, employees, or other differently.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

Yes. Correspondences are issued and applicants are given 30 days (60 days if overseas) to respond to request for additional information, prior to denial of their application. Those applications that are not eligible for certification in accordance with IRM procedure are notified of their right to request Competent Authority Assistance.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?

No. U. S. CERT is not web-based.

[View other PIAs on IRS.gov](#)